

(19)日本国特許庁 (JP)

(12) 公開特許公報 (A)

(11)特許出願公開番号
特開2003-173300
(P2003-173300A)

(43)公開日 平成15年6月20日(2003.6.20)

(51)Int.Cl. ⁷	識別記号	F I	マークコード(参考)
G 0 6 F 13/00	3 5 1	G 0 6 F 13/00	3 5 1 Z 5 B 0 8 5
15/00	3 3 0	15/00	3 3 0 A 5 B 0 8 9
H 0 4 L 12/66		H 0 4 L 12/66	B 5 K 0 3 0

審査請求 未請求 請求項の数15 OL (全16頁)

(21)出願番号	特願2002-93667(P2002-93667)
(22)出願日	平成14年3月29日(2002.3.29)
(31)優先権主張番号	特願2001-295368(P2001-295368)
(32)優先日	平成13年9月27日(2001.9.27)
(33)優先権主張国	日本 (JP)

(71)出願人	000003078 株式会社東芝 東京都港区芝浦一丁目1番1号
(72)発明者	菅野 伸一 神奈川県川崎市幸区小向東芝町1番地 株式会社東芝研究開発センター内
(72)発明者	橋岡 正道 東京都青梅市末広町2丁目9番地 株式会社東芝青梅工場内
(74)代理人	100083161 弁理士 外川 英明

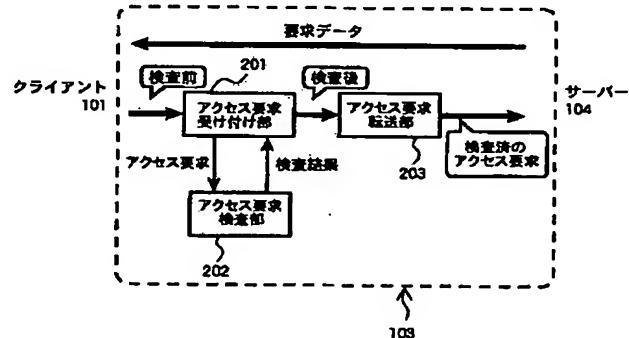
最終頁に続く

(54)【発明の名称】 サーバー計算機保護装置、サーバー計算機保護方法、サーバー計算機保護プログラム及びサーバー計算機

(57)【要約】

【課題】 DoSの攻撃からサーバー計算機を保護するサーバー計算機保護装置を提供する。

【解決手段】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段(201)と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段(202)と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段(203)と、を備えるサーバー計算機保護装置。



【特許請求の範囲】

【請求項1】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項2】 前記アクセス要求検査手段は、前記クライアント計算機が送ってくるアクセス要求パケットが一連の接続要求パケット、確認応答パケット及びデータ要求パケットである場合は、正当なアクセス要求であると判断することを特徴とする請求項1記載のサーバー計算機保護装置。

【請求項3】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段と、前記所定期間にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、

前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段と、

前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項4】 所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、

前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、

前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段と、

前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えるサーバー計算機保護装置。

【請求項5】 パケットのヘッダーを修正するヘッダー修正手段をさらに備え、

前記ヘッダー修正手段は、前記アクセス要求パケットを

前記サーバー計算機へ転送する際に前記アクセス要求パケットのヘッダーを修正することを特徴とする請求項1乃至4記載のサーバー計算機保護装置。

【請求項6】 前記サーバー計算機から前記クライアント計算機への応答を代わりに行う代理応答部をさらに備え、

前記代理応答部は前記クライアント計算機と前記サーバー計算機保護装置との間でコネクションを確立した後に、代理応答を行うことを特徴とする請求項1乃至4記載のサーバー計算機保護装置。

【請求項7】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、

正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項8】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、

前記所定期間にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項9】 所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法。

【請求項10】 クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、
正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、
をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項11】クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間に内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、

前記所定期間に内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項12】所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、

前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、

前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、

前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラム。

【請求項13】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、

前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【請求項14】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、

前記サーバー計算機はサーバー計算機保護装置を含み、

前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間に内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段と、前記所定期間に内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【請求項15】クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、

前記サーバー計算機はサーバー計算機保護装置を含み、

前記サーバー計算機保護装置は、所定のクライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段と、を備えることを特徴とするサーバー計算機。

【発明の詳細な説明】

【0001】

【発明の属する技術分野】本発明は、クライアント計算機とサーバー計算機間のネットワークシステムに関し、特に、意図的にサーバー計算機の処理を妨害する不正なアクセスからサーバー計算機を保護するサーバー計算機保護装置に関する。

【0002】

【従来の技術】近年、インターネット等を利用し、不特定多数あるいは特定多数のクライアント計算機をパケット交換ネットワーク経由でサーバー計算機に接続し、クライアント計算機からの要求に応じてサーバー計算機からデータを供給することを目的とする計算機サーバーシステムが広く使われている。ここで、パケットとは、ネットワーク上を流れるひとたまりのデータをいい、大まかに分けると、ヘッダーとデータ本体で構成されている。さらに、ヘッダー内には、送信先のIP(Internet Protocol)アドレス、宛先のIPアドレス、パケットの

50

前後関係を表す伝送シーケンス番号等から構成されている。

【0003】しかしながらこのようなシステムの妨害を意図した不正なアクセスによる攻撃が増加する傾向にある。

【0004】特に、一つのクライアント計算機から同時に大量に同じようなアクセス要求をサーバー計算機に対して行うことによって、標的となるサーバー計算機のデータ供給サービスを不能にする攻撃方法(以下、DoS攻撃(Denial of Service attack)と表記)は、正当なクライアントからのアクセスとの区別がつきにくく有効な対策をとることが困難である。尚、このDoS攻撃を複数のクライアント計算機が行う場合をDDoS攻撃(Distributed Denial of Service attack)という。

【0005】ここで、クライアント計算機からサーバー計算機への正当なアクセス要求とは、実際にサーバー計算機からデータを受け取ったアクセス要求をいう。TCP/IP(Transmission Control Protocol/IP)プロトコルにおける正当なアクセス要求の一例としては、クライアント計算機はサーバー計算機へ接続要求パケット(SYN(SYNchronousness)パケット)を送り、サーバー計算機はクライアント計算機へ接続要求確認パケット(SYN+ACK(ACKnowledgement)パケット)を送り、クライアント計算機はサーバー計算機へ確認応答パケット(ACKパケット)を送ることによって、論理的な通信路(コネクション)が確立する(3ウェイ・ハンドシェーク方式)。このコネクション確立(Established)状態で、クライアント計算機はサーバー計算機へデータ要求パケット(URL(Uniform Resource Locator)パケット)を送り、サーバー計算機はクライアント計算機へURLパケットによって要求されたデータパケットを送り、実際にクライアント計算機が受け取るという手順がある。

【0006】インターネットにおけるこのようなDoS攻撃の一般的な方法としては、以下のようない妨害方法が挙げられる。

【0007】(1) SYNパケットのみをサーバー計算機の処理能力を超えるぐらい大量に送りつけ、サーバー計算機がSYN+ACKパケットを送れないようにする方法(以下SYN floodと表記)

(2) SYNパケット及びACKパケットを大量にサーバー計算機へ送り、このサーバー計算機との間でコネクションを確立したが、その後URLパケットを一定時間以内に送らず放置する方法(以下Established floodと表記)

(3) 通常のクライアントと同様にコネクション確立状態でURLパケットを送る正当なアクセスだが、この正当なアクセスを大量に行うことによって、意図的にサーバー計算機の処理を妨害する方法(例えば、予め決めた時間に、たくさんの人が特定のサーバー計算機にアクセスする場合; DDoS攻撃)(以下、Accessfloodと表記)

このような攻撃をサーバー計算機が受けると、接続要求

毎にデータ供給用メモリを確保するためにサーバー計算機内の記憶装置等の資源を浪費してしまい、妨害を意図していないクライアント計算機からの通常のアクセスが大きく滞ることになる。

【0008】そこで、これらの攻撃からサーバー計算機を保護する目的で、サーバーとネットワークの間に配置するサーバー計算機保護装置においては、SYN floodに対しても、複数回の接続要求が繰り返されたもののみを正当な接続要求として処理したり、既に正当なアクセス

10 があったクライアントからのアクセスを正当な接続要求として処理し、それ以外のアクセスについてはパケットを破棄する方法などが従来取られている。

【0009】しかし、このような方法では攻撃側が複数回の同じ接続要求を出したりする方法を取ることにより攻撃が成立するという問題点があり、また Established flood や Access flood については対抗することができないという問題がある。

【0010】

【発明が解決しようとする課題】DoS攻撃に対し、これらの攻撃の影響からサーバー計算機を保護し、正当なしかも妨害を意図していないクライアントからのサービスを大きく滞らせることなく行うことを課題とする。

【0011】

【課題を解決するための手段】第1の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段(201)と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段(202)と、前記アクセス要求検査手段30 によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段(203)と、を備えるサーバー計算機保護装置である。

【0012】第2の発明は、前記アクセス要求検査手段は、前記クライアント計算機が送ってくるアクセス要求パケットが一連の接続要求パケット、確認応答パケット及びデータ要求パケットである場合は、正当なアクセス要求であると判断することを特徴とする第1の発明記載のサーバー計算機保護装置である。

【0013】第3の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段(201)と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段(303)と、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段(301)と、前記データ供給数計測手段50 及び接続要求数計測手段の出力結果を用いて前記サーバ

一計算機の負荷状態を検査するサーバー負荷検査手段（302）と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（203）と、を備えるサーバー計算機保護装置である。

【0014】第4の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるアクセス要求受け付け手段（201）と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（301）と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段（302）と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（203）と、を備えるサーバー計算機保護装置である。

【0015】第5の発明は、パケットのヘッダーを修正するヘッダー修正手段（210）をさらに備え、前記ヘッダー修正手段は、前記アクセス要求パケットを前記サーバー計算機へ転送する際に前記アクセス要求パケットのヘッダーを修正することを特徴とする第1乃至第4の発明記載のサーバー計算機保護装置である。

【0016】第6の発明は、前記サーバー計算機から前記クライアント計算機への応答を代わりに行う代理応答部（501）をさらに備え、前記代理応答部は前記クライアント計算機と前記サーバー計算機保護装置との間でコネクションを確立した後に、代理応答を行うことを特徴とする第1乃至第4の発明記載のサーバー計算機保護装置である。

【0017】第7の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【0018】第8の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステッ

プと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【0019】第9の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、を備えるサーバー計算機保護方法である。

【0020】第10の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するステップと、正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【0021】第11の発明は、クライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記アクセス要求パケット内の接続要求パケットを受け付けるのに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数である接続要求数を計測するステップと、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記接続要求数及びデータ供給数を用いて前記サーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【0022】第12の発明は、所定のクライアント計算機から送られてくるアクセス要求パケットをサーバー計算機の代わりに受け付けるステップと、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数であるデータ供給数を計測するステップと、前記データ供給数を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するステップと、前記サーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するステップと、をコンピュータに実行させるためのサーバー計算機保護プログラムである。

【0023】第13の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であつ

て、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（201）と、受け付けたアクセス要求パケットが正当なアクセス要求であるか否かを検査するアクセス要求検査手段（202）と、前記アクセス要求検査手段によって正当なアクセス要求であると認められたアクセス要求パケットのみ前記サーバー計算機へ転送するアクセス要求転送手段（203）と、を備えることを特徴とするサーバー計算機である。

【0024】第14の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、前記クライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（201）と、前記アクセス受け付け手段が前記アクセス要求パケット内の接続要求パケットを受け付けるに対応して、所定期間内に全てのクライアント計算機から届いた接続要求パケットの数を計測する接続要求数計測手段（303）と、前記所定期間内にサーバー計算機からクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（301）と、前記データ供給数計測手段及び接続要求数計測手段の出力結果を用いて前記サーバー計算機の負荷状態を検査するサーバー負荷検査手段（302）と、前記サーバー負荷検査手段によってサーバー計算機の負荷が所定の基準値以下と判断された場合は、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（203）と、を備えることを特徴とするサーバー計算機である。

【0025】第15の発明は、クライアント計算機からの要求に応じたデータを供給するサーバー計算機であって、前記サーバー計算機はサーバー計算機保護装置を含み、前記サーバー計算機保護装置は、所定のクライアント計算機から送られてくるアクセス要求パケットを前記サーバー計算機の代わりに受け付けるアクセス要求受け付け手段（201）と、前記サーバー計算機が前記所定のクライアント計算機へデータ供給している数を計測するデータ供給数計測手段（301）と、前記データ供給数計測手段の出力結果を用いて、前記所定のクライアント計算機に対するサーバー計算機の負荷状態を検査するサーバー負荷検査手段（302）と、前記サーバー負荷検査手段によって前記所定のクライアント計算機に対するサーバー計算機の負荷が所定の基準値以下と判断された場合、前記アクセス要求パケットを前記サーバー計算機へ転送するアクセス要求転送手段（203）と、を備えることを特徴とするサーバー計算機である。

【0026】

【発明の実施の形態】以下、本発明の実施の形態について図面を参照しながら説明する。

【0027】図1は、本発明の実施形態に係るサーバー計算機保護装置が適用されるネットワークシステムの概要図である。サーバー計算機104は、サーバー計算機保護装置103を介してネットワーク102に接続されており、また、このネットワーク102に接続されているクライアント計算機101とのデータパケットのやり取りには必ずサーバー計算機保護装置が仲介している。

10 【0028】（第1の実施の形態）図2は、第1の実施形態に係るサーバー計算機保護装置103のブロック図である。保護装置103は、アクセス要求受け付け部201と、アクセス要求検査部202と、アクセス要求転送部203を含んでいる。

【0029】クライアント計算機101からのアクセス要求つまり検査前のアクセス要求はアクセス要求受け付け部201で受け取り、その後アクセス要求検査部202に転送される。アクセス要求のパケットには、接続要求パケット（SYNパケット）、確認応答パケット（ACKパケット）及びデータ要求パケット（URLパケット）の3段階のパケットがある。

【0030】検査結果はアクセス要求受け付け部201に入り、検査後のアクセス要求がアクセス要求転送部203に送られる。そして、検査済のアクセス要求がアクセス要求転送部203からサーバー計算機104へ出力される。

【0031】以下、保護装置103全体の処理の流れを図3のフローチャートを用いて説明する。保護装置103は、クライアント計算機101から接続要求パケット（SYNパケット）を受け取ると、クライアント計算機へS YN+ACKパケットを送り（S101）、次の段階のアクセス要求（ACKパケットまたはURLパケット）待ち状態になる（S102）。

【0032】そして、不正アクセスか否かを判断する（S103）。判断の一例としては、クライアント計算機101からのアクセス要求は、保護装置103内のアクセス要求受け付け部201により受領し、アクセス要求検査部202でアクセス要求の内容を検査する。本実施形態で検査できる不当なアクセス要求は、従来の技術で説明したSYN floodとEstablished floodの2種類である。そして、正当なアクセス要求とはコネクション確立状態で一定時間以内にURLパケットを送ってくる場合をいう。

【0033】検査の結果、正当なアクセス要求だと認められた場合、アクセス要求転送部203はサーバーと接続し（S104）、正当なアクセス要求をサーバー計算機104に転送する（S105）。そして、サーバー計算機104はURLパケットによって指定されたデータをパケット単位で保護装置103を介してクライアント計算機101に供給する（S106）。保護装置103は

データの供給が完了してからサーバー計算機104との接続を切断し(S107)、クライアント計算機101との接続も切断する。一方、不当なアクセス要求であると判断した場合は、S103からすぐにS108のクライアントとの切断処理が実行される。

【0034】したがって、従来の技術で説明したSYN flood, Established flood等のDoS攻撃からサーバー計算機を保護できる。

【0035】尚、アクセス要求検査部202の正当なアクセス要求であるか否かの判断基準としては、上述したようなSYNパケットのみを送りつけてくるようなアクセス要求が所定の伝達形式から外れていないかどうかの他に、サーバー計算機104にはありえないアクセス(例えば、不当なURLパケット)を要求しているかどうか等がある。

【0036】本実施形態の変形例としては、検査前の全段階のアクセス要求はアクセス要求受け付け部201に入ると同時に、アクセス要求転送部203にも送られ、データ要求検査部202の検査結果をデータ要求転送部203が受け取ってから、サーバー計算機104へアクセス要求を出力しても良い。

【0037】(第2の実施の形態)図4は第2の実施形態に係るサーバー計算機保護装置103のブロック図である。本実施形態の特徴は、第1の実施形態で説明したアクセス要求の内容を検査するアクセス要求検査部の代わりに、クライアント計算機101から送られてくる接続要求パケット(SYNパケット)の数が所定の値を超えた場合、すなわち、サーバー計算機104の負荷が過大になった場合には、サーバー計算機104へアクセス要求を転送するのを止めることである。

【0038】クライアント計算機101からのあるSYNパケットをデータ要求受け付け部201及び接続要求数計測部303により受け取る。データ供給数計測部301は、常にサーバー計算機104が所定時間に供給するデータ供給数を計測する。ここで、接続要求数はある接続要求を受け付けたときに全てのクライアント計算機から届いたSYNパケットの総数をいい、通常、一つのクライアント計算機とサーバー計算機との間には複数のコネクションが張られる。また、データ供給数とは、成立しているコネクションのうち、ある接続要求を受け付けたときに実際にデータ供給している数をいう。

【0039】以下、保護装置103全体の処理の流れを図5(a)のフローチャートを用いて説明する。保護装置103は接続要求待ち(S201)の状態から、接続要求数計測部303でクライアント計算機101からのSYNパケットを検知すると、サーバー負荷検査部302はデータ供給数計測部301及び接続要求数計測部303の出力結果を用いて、サーバー計算機104の負荷が過大か否かを検査する(S202)。判断基準の一例としては、データ要求数(URLパケットの総数)に比べて

データ供給数が少ないと負荷が過大であるが挙げられる。

【0040】所定の負荷を超えていない場合には、クライアント計算機と接続し(S203)、データ要求待ち(S204)状態となる。この時、サーバー負荷検査部302は接続数を1増加させる(S205)。

【0041】続いて、サーバーと接続し(S206)、クライアント計算機103からのデータ要求パケットをサーバーに転送する(S207)。そして、サーバー計算機104がクライアント計算機にデータを供給してから(S208)、保護装置103はクライアント計算機101及びサーバー計算機104との接続を切断し(S209)、サーバー負荷検査部302は接続数を1減少させる(S210)。

【0042】一方、所定の負荷を超えていた場合には接続要求待ちの状態(S201)に戻る。これにより、DoS攻撃によってサーバーの負荷が過大になるのを防止し、サーバーの処理速度低下を防止することができる。

【0043】図5(b)は、同図(a)のS202で所定の負荷を超えていた場合の変形例である。すなわち、S202で所定の負荷を超えていた場合(所定の接続数を超えていた場合)であって、保護装置103が処理できる接続数を超える場合には、接続処理が完了していないコネクションのうち最も古いものを破棄してから(S202'のy)、クライアント計算機と接続する(S203)。以降の処理は、同図(a)と同じである。一方、S202で所定の負荷を超えている場合であるが、保護装置103が処理できる接続数を超えていない場合には、接続要求待ちの状態(S201)に戻る。このように、コネクションのうち最も古いものを破棄することによって、保護装置自体へDoS攻撃を受けた時でもサービスを続行できる。

【0044】(第3の実施の形態)図6は、第3の実施形態に係るサーバー計算機保護装置103のブロック図である。図7は本実施形態に係るフローチャートである。本実施形態はアクセス要求を送ってきたクライアント計算機毎にデータ供給数計測部301及びサーバー負荷検査部302を設けることを特徴とする。

【0045】まず、保護装置103は、接続要求待ちの状態(S301)から、特定のクライアント計算機からSYNパケット及びACKパケットを受けると、前記特定のクライアント計算機との間でコネクションを張り(S302)、前記特定のクライアント計算機専用のデータ供給数計測部301及びサーバー負荷計算部302(以下、本実施形態に限ってデータ供給数計測部301及びサーバー負荷計算部302と省略する)を設ける。尚、データ供給数計測部301及びサーバー負荷計算部302は、単純な計算機能を有していれば良いので、保護装置103のメモリ及びCPUの消費は少ない。したがって、クライアント計算機毎に1000~10000個ぐ

らい設けることができる。

【0046】次に、前記特定のクライアント計算機からのアクセス要求待ちの状態になり(S304)、前記特定のクライアント計算機からアクセス要求が来ると、アクセス要求受け付け部201からすぐにアクセス要求伝達部203へ行き、サーバー計算機104とコネクションを張る(S305)。

【0047】データ供給数計測部301は、現在サーバー計算機104が伝送中の要求されたデータを送付した特定のクライアント計算機へのデータ供給状況を計測することによって、特定のクライアント計算機に対するサーバーの負荷が過大か否かを判断する(S306)。所定の負荷を超えていない場合には、サーバー負荷検査部302は、アクセス要求転送部203へサーバー計算機104にURLパケットを転送するように指示をし(S307)、サーバー計算機104が要求されたデータを特定のクライアント計算機に供給し(S308)、データ供給が完了したら特定のクライアント計算機及びサーバー計算機との接続を切断する。

【0048】一方、所定の負荷を超えていた場合には、データ要求転送部203がデータ要求パケットをサーバー計算機104に転送するのを保留するために再度S306の処理を行い、特定のクライアント計算機へのデータ供給数が減少するのを待つ。

【0049】これにより、サーバー計算機104の負荷が過大になるのを防止するとともに、特定のクライアント計算機によるサーバー計算機104の独占状態を回避し、他のクライアント計算機へのデータ供給を阻害されることを減少できる。したがって、従来の技術で説明したAccess floodに対応することもできる。

【0050】(第4の実施の形態)図8は、第4の実施形態に係るサーバー計算機保護装置103のブロック図であり、本実施形態は、第1の実施形態と基本的に同じであるが、ヘッダー修正部210を備えていることを特徴とする。

【0051】例えばTCP/IPでは、接続処理にあたりヘッダー内に、伝送シーケンス番号を付与しパケットの前後関係を制御している。接続開始にあたってこれらは受送双方にてサーバー計算機とクライアント計算機のやりとりで決定される。

【0052】しかし、本実施形態を利用する場合にはサーバー計算機104への接続動作(図3のS104)はデータ要求の正当性の検査後になる(図3のS103)ので、保護装置103が任意に発生した保護装置用シーケンス番号でクライアント計算機101と接続処理を行わざるをえない(図3のS101)。この保護装置用シーケンス番号は検査後に行われるサーバー計算機との接続処理(図3のS104)においてサーバー計算機104から通知されるサーバー計算機用シーケンス番号と異なるため、そのまま要求されたデータのパケットを伝送

するとTCP/IPプロトコルを使用したデータ伝送が不可能である。そこで、ヘッダー修正部210を用いこれらのシーケンス番号の差分を修正し、また他のヘッダー情報(例えば送信先のIPアドレス、宛先のIPアドレス)を必要があれば整合が取れるように修正することによりサーバー計算機104からクライアント計算機101への通信を成立させることができる。

【0053】一例としては、一つのデータ要求に対して以下の～の処理を行っている。

10 【0054】クライアント計算機101からの接続要求をデータ要求受け付け部201、データ要求検査部202及びデータ転送伝達部203によって検査後に、クライアント計算機101とサーバー計算機104とのコネクションを確立する。

【0055】このコネクションを経由して送られてくるクライアント計算機101からのデータ要求パケットのヘッダーをヘッダー修正部210で修正してから、サーバー計算機104へ転送する。

20 【0056】このコネクションを経由して送られてくるサーバー計算機104からのデータパケットのヘッダーをヘッダー修正部210で修正してから、クライアント計算機101へ転送する。

【0057】(第5の実施形態)図9は、第5の実施形態に係るサーバー計算機保護装置103のブロック図である。本実施形態は、第2の実施形態と基本的に同じであるが、第4の実施形態で説明したヘッダー修正部210を備えていることを特徴とする。

30 【0058】尚、ヘッダー修正部210がハッシュ関数を用いてクライアント計算機101とサーバー計算機104とのコネクションを管理する方法を利用した場合には、図5のS202の代わりに、該ハッシュのテーブルが溢れたことをもってサーバー計算機104の負荷を過大であると判断しても良い。

【0059】(第6の実施形態)図10は、第6の実施形態に係るサーバー計算機保護装置103のブロック図である。本実施形態は、第3の実施形態と基本的に同じであるが、第4の実施形態で説明したヘッダー修正部210を備えていることを特徴とする。

40 【0060】(他の実施形態)本発明は上記実施形態に限定されるものではなく、本発明の趣旨を逸脱しない範囲内で適宜変更できる。以下、変形例について説明する。

【0061】(変形例1)図11は、変形例1に係るサーバー計算機保護装置103のブロック図である。本変形例は、第6の実施形態の変形例であり、保護装置103とサーバー計算機104との接続数を計測するサーバー接続数計測部401を備えていることを特徴とする。このサーバー接続数計測部401の出力結果はクライアント計算機毎に設けられたサーバー負荷検査部302に入力されている。また、クライアント計算機毎の接続数

は、クライアント計算機毎に設けられたデータ供給数301で計測できる。したがって、いずれの接続数も保護装置103内部で計測できるので、クライアント計算機毎のサーバー負荷検査処理も簡易化できる。

【0062】(変形例2)変形例2は、第4の実施形態の変形例であり、保護装置103には、クライアント計算機との間でコネクション成立後、データ要求パケットが届くまでの時間を計測する時計部を有している。そして、この時計部を用いて、データ要求受け付け部201が予め規定した時間の間に所定の形式のデータ要求が届かない場合には不正なアクセスと判断し、コネクションを破棄する。これによりサーバー計算機保護装置内部の資源が過大になることを防ぎ、なおかつ正当なクライアントからの接続動作に早い段階でメモリーなどの資源を振り向けることができるようになる。

【0063】また、上述した時計部を用いて、データ要求受け付け部201はコネクションを確立してから最も経過時間が長いものを不正なアクセスと判断して、コネクションを破棄しても良い。

【0064】さらに、データ要求受け付け部201は、上述した時計部を用いて一定時間内に同一クライアントからの同一データに対する要求回数を計測する機能を有すれば、この計測し、あらかじめ設定した一定時間内の同一データ要求回数の限度を超えた場合に不正なアクセスとして判断して、コネクションを破棄しても良い。

【0065】(変形例3)図12及び図13は、変形例3に係るサーバー計算機保護装置103のブロック図及びフローチャートである。本変形例は、他の実施形態に適用可能であり、サーバー計算機104の代りにクライアント計算機101へ応答する代理応答部501を備えていることを特徴とする。代理応答部501がサーバー計算機104に成り代わるためにには、図8で説明したヘッダー修正部210を備えていればよい。

【0066】クライアント計算機101と保護装置103とがTCP/IPプロトコルでコネクションを確立する手順は上述した通りである(S401～S404)。その後(、すなわち、クライアント計算機101からのデータ要求が来る前)に、代理応答部501は、サーバー計算機104からクライアント計算機101への応答を代わりに行う(S405)。

【0067】ここでの応答とは、TCP/IPの上位プロトコル、例えば、SMTP(Simple Mail Transfer Protocol)の場合は、サーバー計算機104がメールを受け取ることが可能であるという状態を示す応答であり、また、POP(Post Office Protocol)の場合には、POPのバージョン(例えば、POP3)を応答する。そして、応答の具体例としては、サーバー計算機104が正常動作している場合にクライアントに返答する内容と同等のもの、あるいは、保護装置103とサーバー計算機104との間で直前に行われた上位プロトコルによる接続動作によりサー

バーカー計算機104が返答したものと同様の内容のものが挙げられる。

【0068】この応答を受けることによって、クライアント計算機101は、サーバー計算機104と上位プロトコルで接続動作が行われたと判断し、データ転送要求等の次の動作に移行する。

【0069】クライアント計算機101からのデータ要求は、要求受付部201で受け付け、要求検査部202でデータ要求の内容を検査した後に、サーバー計算機104に伝達する。サーバー計算機104は、伝達された内容に基づき所定のデータをクライアント計算機101に返送する。その後、上述した切断手順を行う(S406～S417)。ここで検査としては、データ要求が所定の伝達形式から外れていないかどうか、ありえないデータを要求しているかどうか等が挙げられる。

【0070】尚、上述したように、クライアント計算機101からのデータ要求が正常であった場合には、保護装置103はサーバー計算機104に接続動作を行い、クライアント計算機101の要求をサーバー計算機104に伝達する。この接続後にサーバー計算機104が応答するものには、先に保護装置103がサーバー計算機104に応答したものと重複する場合がある。それゆえ、データ要求の処理に齟齬を来さない場合にはこの応答をクライアントに伝達しない。もし、齟齬を来す場合には保護装置103はサーバー計算機104とクライアント計算機101との接続を破棄する処理を行う。

【0071】他の変形例としては、上述したサーバー計算機保護装置はサーバー計算機の中に含まれていても良い。この場合、サーバー計算機保護装置専用のメモリ等のハードウェアがサーバー計算機内にあれば良い。

【0072】(記録媒体への適用)また、本実施形態における処理をコンピュータで実行可能なプログラムで実現し、このプログラムをコンピュータで読み取り可能な記憶媒体として実現することも可能である。

【0073】なお、本記憶媒体としては、磁気ディスク、フレキシブルディスク、ハードディスク、光ディスク(CD-ROM, CD-R, DVD等)、光磁気ディスク(MO等)、半導体メモリ等、プログラムを記憶でき、かつコンピュータが読み取り可能な記憶媒体であれば、その記憶形式は何れの形態であってもよい。

【0074】また、記憶媒体からコンピュータにインストールされたプログラムの指示に基づきコンピュータ上で稼動しているOS(オペレーションシステム)や、データベース管理ソフト、ネットワーク等のMW(ミドルウェア)等が本実施形態を実現するための各処理の一部を実行してもよい。

【0075】さらに、本記憶媒体は、コンピュータと独立した媒体に限らず、LANやインターネット等により伝送されたプログラムをダウンロードして記憶または一時記憶した記憶媒体も含まれる。

【0076】また、記憶媒体は1つに限らず、複数の媒体から本実施形態における処理が実行される場合も、本発明における記憶媒体に含まれ、媒体の構成は何れの構成であってもよい。

【0077】なお、上記コンピュータは、記憶媒体に記憶されたプログラムに基づき、本実施形態における各処理を実行するものであって、パソコン等の1つからなる装置、複数の装置がネットワーク接続されたシステム等の何れの構成であってもよい。

【0078】また、上記コンピュータとは、パソコンに限らず、情報処理機器に含まれる演算処理装置、マイコン等も含み、プログラムによって本実施形態の機能を実現することが可能な機器、装置を総称している。

【0079】

【発明の効果】上述したように本発明によれば、DoS攻撃に対し、これらの攻撃の影響からサーバー計算機を保護し、正当なしかも妨害を意図していないクライアントからのサービスを大きく滞らせることなく行うことができる。

【図面の簡単な説明】

【図1】 本発明の実施形態に係るサーバー計算機保護装置が適用されるネットワークシステムの概要図。

【図2】 本発明の第1の実施形態に係るサーバー保護装置のブロック図。

【図3】 第1の実施形態に係るフローチャート。

【図4】 本発明の第2の実施形態に係るサーバー保護装置のブロック図。

【図5】 第2の実施形態に係るフローチャート。

【図6】 本発明の第3の実施形態に係るサーバー保護装置のブロック図。

【図7】 第3の実施形態に係るフローチャート。

【図8】 本発明の第4の実施形態に係るサーバー保護装置のブロック図。

【図9】 本発明の第5の実施形態に係るサーバー保護装置のブロック図。

【図10】 本発明の第6の実施形態に係るサーバー保護装置のブロック図。

10 【図11】 本発明の変形例1に係るサーバー保護装置のブロック図。

【図12】 本発明の変形例3に係るサーバー保護装置のブロック図。

【図13】 本発明の変形例3に係るフローチャート。

【符号の説明】

101 クライアント計算機

102 ネットワーク

103 サーバー計算機保護装置

20 104 サーバー計算機

201 データ要求受け付け部

202 データ要求検査部

203 データ要求転送部

301 データ供給数計測部

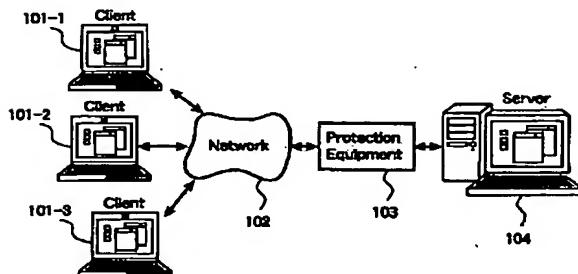
302 サーバー負荷検査部

303 接続要求数計測部

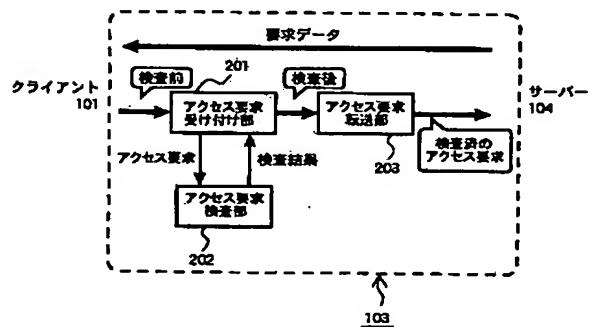
401 サーバー接続数計測部

501 代理応答部

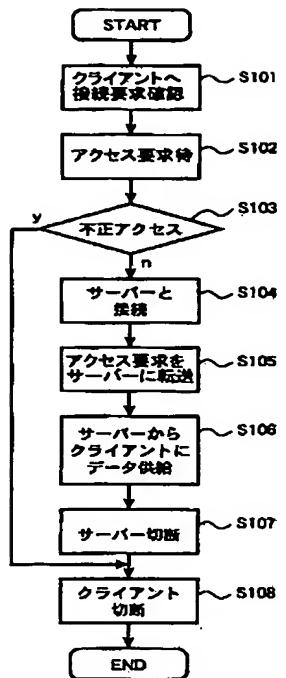
【図1】



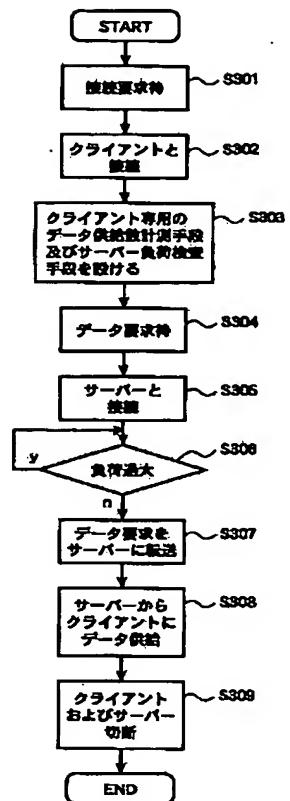
【図2】



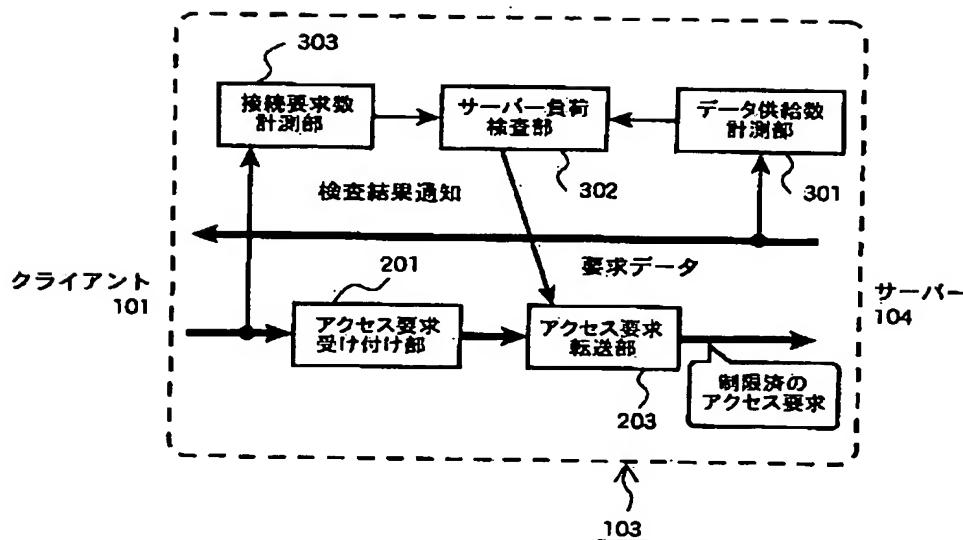
【図3】



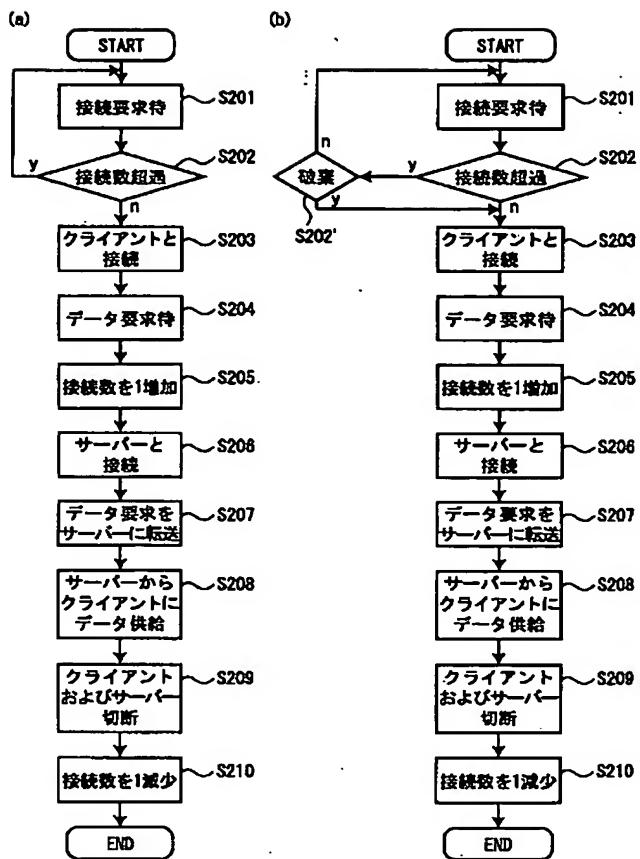
【図7】



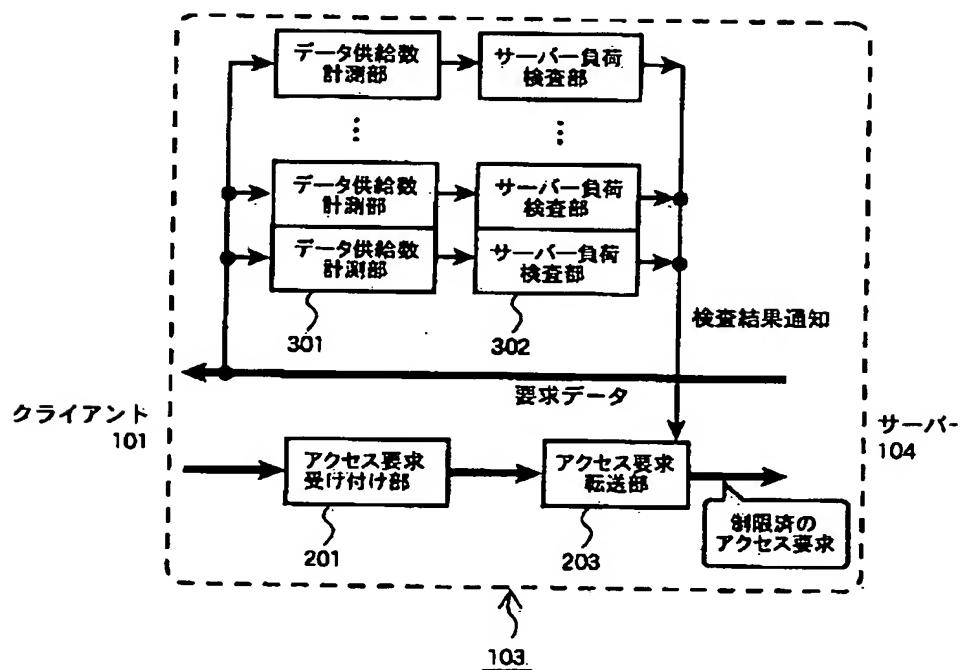
【図4】



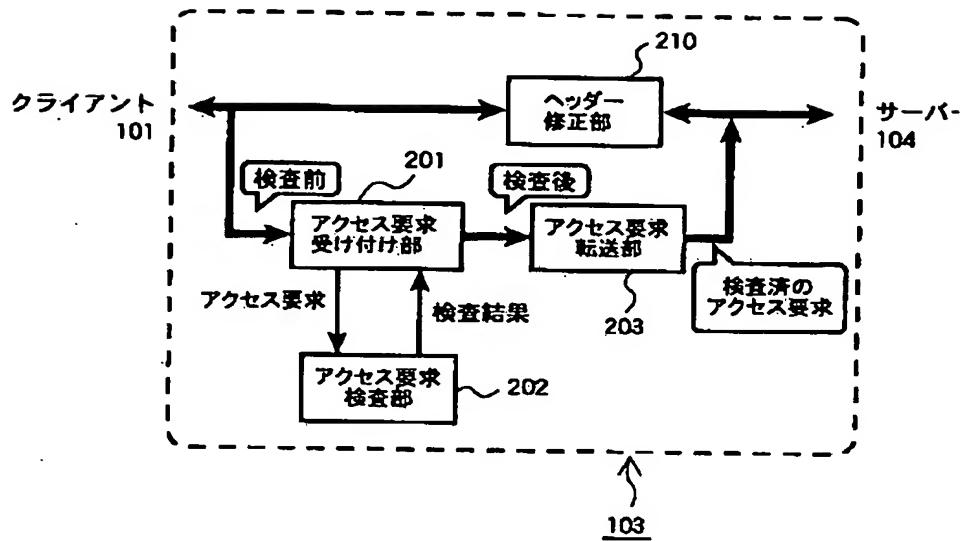
【図5】



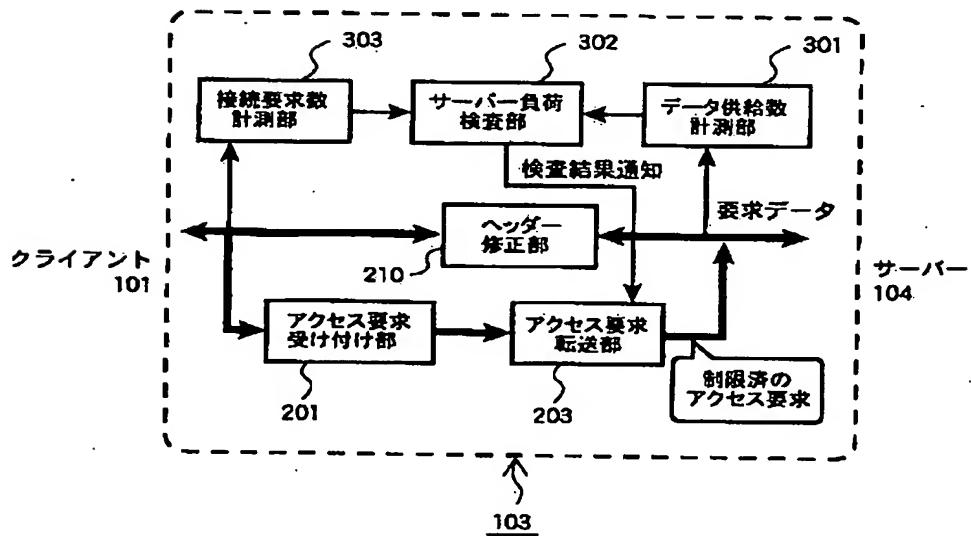
【図6】



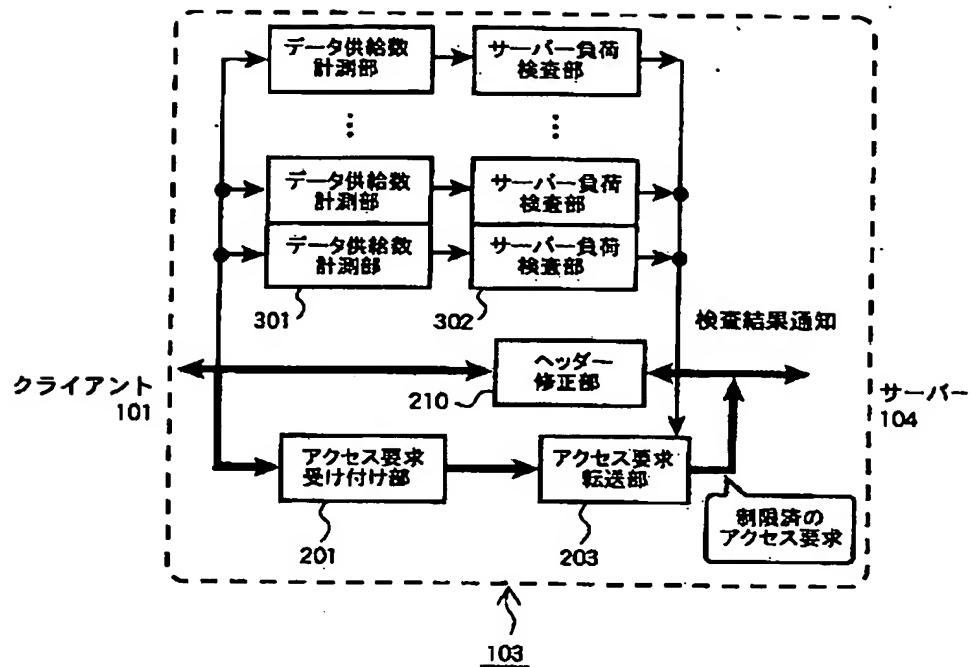
【図8】



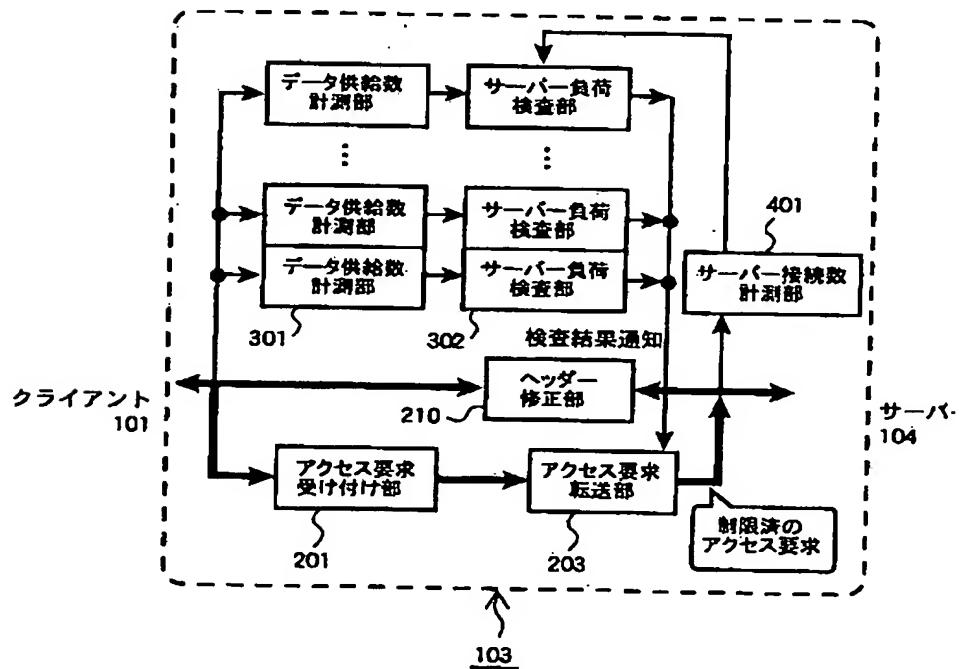
【図9】



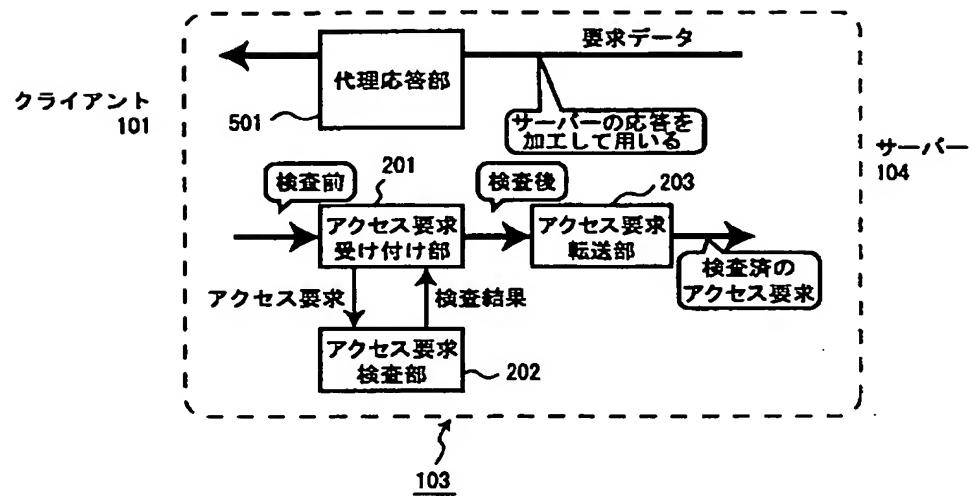
【図10】



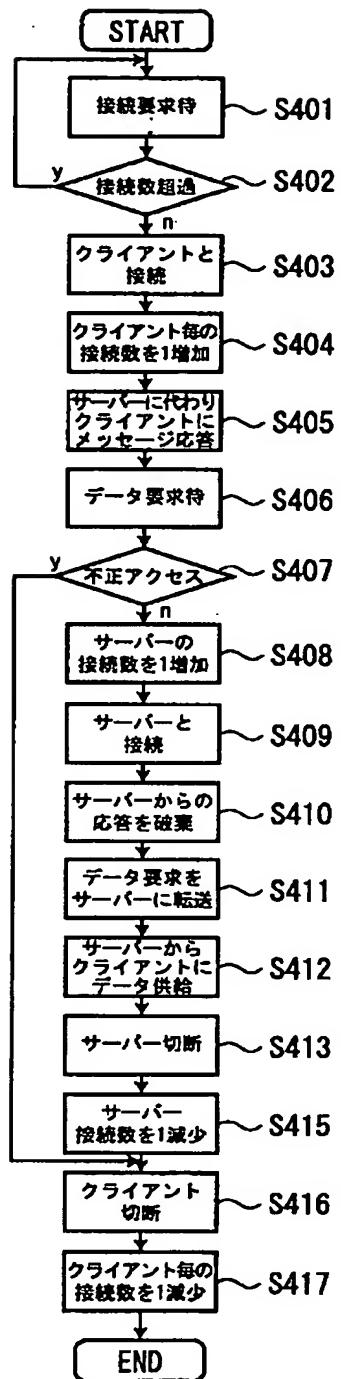
【図11】



【図12】



【図13】



フロントページの続き

Fターム(参考) 5B085 AE00 BA06 BG07
 5B089 GA11 GA19 GB01 GB02 KA06
 KA17 KB13 MA07
 5K030 GA15 MB09